What is claimed is:

1. A method of internally encrypting data in a relational database, comprising the steps of:

providing a security dictionary comprising one or more security catalogs;

receiving data from a user;

associating said data with a database column and at least one authorized user;

generating a working encryption key;

internally encrypting said working encryption key using a public key from an authorized user;

storing said encrypted working key in a security catalog; and

using said working key to internally encrypt said data.

2. The method of claim 1 further comprising the step of generating a private key needed to decrypt said encrypted working key.

3. The method of claim 2 wherein said public key is a password and is used by the system to look up said private key.

4. The method of claim 1 wherein said step of associating said data with a database column and a user is accomplished with an extended SQL syntax and further comprises the step of creating a relational database object comprising:

the identity of said authorized users;

a relational database table;

the identity of said column within said relational database table; and

one or more security flags, said flags indicating user privileges to access said data.

5. The method of claim 1 wherein said working key is provided by a user.

6. The method of claim 1 wherein said working key is randomly generated.

7. The method of claim 1 further comprising the steps of:

receiving a query and private key from a user;

checking the ownership of an encrypted column using said security catalog to verify the user is authorized;

internally decrypting said encrypted working encryption key with said private key;

internally decrypting said encrypted column with said working key;

processing said query; and

returning an answer to said query to the user.

8. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for internally encrypting data in a relational database, said method steps comprising:

providing a security dictionary comprising one or more security catalogs;

receiving data from a user;

associating said data with a database column and at least one authorized user;

generating a working encryption key;

internally encrypting said working encryption key using a public key from an authorized user;

storing said encrypted working key in a security catalog; and

using said working key to internally encrypt said data.

9. The invention of claim 8 further comprising the step of generating a private key needed to decrypt said encrypted working key.

10. The invention of claim 9 wherein said public key is a password and is used by the system to look up said private key.

11. The invention of claim 8 wherein said step of associating said data with a database column and a user is accomplished with an extended SQL syntax and further comprises the step of creating a relational database object comprising:

the identity of said authorized users;

a relational database table;

the identity of said column within said relational database table; and

one or more security flags, said flags indicating user privileges to access said data.

12. The invention of claim 8 wherein said working key is provided by a user.

13. The invention of claim 8 wherein said working key is randomly generated.

14. The invention of claim 8 further comprising the steps of:

receiving a query and private key from a user;

checking the ownership of an encrypted column using said security catalog to verify the user is authorized;

internally decrypting said encrypted working encryption key with said private key;

internally decrypting said encrypted column with said working key;

processing said query; and

returning an answer to said query to the user.